REMARKS

In the Office Action dated January 14, 2004, The Examiner noted that the Declaration filed with the original application papers did not include an indication of the filing date or the Serial No. This is of course true, because the Declaration was filed with the original application papers, and at the time that Declaration was prepared, neither the filing date nor the Serial No. were known. The patent rules recognize that this will not be an unusual situation, and therefore merely require that the Declaration identify the application to which it is directed (37 C.F.R. §1.63(b)(1). The Declaration filed in the present application is based on the approved Declaration form appearing in MPEP Section 602, which specifically includes the alternatives of designating the application by attachment to the Declaration or by designating the Serial No. and filing date. Moreover, in the third and fourth paragraphs under MPEP Section 605.04(a), the definition of "attached" is provided, clearly indicating that attachment is one of the options for properly identifying the application.

It is true that MPEP Section 602.02 requires that when a *new* or *substitute* oath or declaration is filed, it must refer to the serial number and filing date. This is logical because the requirement for a new or substitute declaration can only be made after the application has been filed, at which time the serial number and filing date are known. The absence of a Serial No. and filing date, by themselves, is not a basis for requiring a new or substitute oath or declaration.

The Declaration used in the present application is the same Declaration that the undersigned counsel has used without objection for filing thousands of patent applications, and Applicants respectfully submit the Examiner has no statutory basis for requiring correction thereof.

Claims 1 and 3 were rejected under 35 U.S.C. §102(e) as being anticipated by Sedlak et al. Claim 2 was rejected under 35 U.S.C. §103(a) as being unpatentable over Sedlak et al in view of Selph et al. Claims 4-8 were rejected under 35 U.S.C. §103(a) as being unpatentable over Sedlak et al in view of Higuchi. Claim 9 was rejected under 35 U.S.C. §103(a) as being unpatentable over Sedlak et al in view of Mori et al. Claims 10, 12 and 13 were rejected under 35 U.S.C. §103(a) as being unpatentable over Sedlak et al in view of Mori et al. Claim 11 was rejected under 35 U.S.C. §103(a) as being unpatentable over Sedlak et al in view of Mori et al, further in view of Higuchi.

These rejections are respectfully traversed for the following reasons. Independent method claim 1 describes steps involving three different functions respectively undertaken by the first function unit, the second function unit and the third function unit for monitoring proper insertion of the security module on a motherboard. As a first observation, Applicants submit that the Sedlak et al reference, which is directed to a chip card that is insertable in a chip card reader, does not involve monitoring insertion of any components on a motherboard. All of the components shown in Figure 2 of the Sedlak et al reference are a part of an integrated circuit component, but even if this component is considered to have, or represent, a "motherboard," there is no component that is removed from, or replaced on, such a motherboard. The chip card disclosed in the Sedlak et al reference is merely inserted into contacts of a chip card reader. This is the normal, intended operation of a chip card, however, and therefore removal of the chip card from the chip card reader cannot be considered any sort of unusual event associated with the use of the chip card. This is in contrast to usage of a security module, which is

intended to provide security for the overall device in which it is inserted. In the context of a security module, therefore, it is highly relevant to assume that if and when the security module is removed from its motherboard, without a proper authorization, this removal constitutes an effort at compromising the security of the device (tampering).

The circuit in the chip card disclosed in the Sedlak et al reference does include a voltage monitoring circuit, however, the details of how this voltage monitoring circuit operates are not made clear in the Sedlak et al reference. It is stated at column 6, lines 22-25, that the voltage detector circuit 20 detects when the supply voltage (which is detected across lines GND and V_{cc} in Figure 2 of Sedlak et al) exceeds or falls below the predetermined upper or lower limit values of the operating voltage, a signal is supplied to the trigger circuit 18 which, in turn, erases the contents of the RAM8. Although it is not explicitly stated in the Sedlak et al reference, the situation of no voltage being present across the lines GND and V_{cc} must be within the aforementioned predetermined limits, otherwise this would result in an erasure of the contents of the RAM8 every time the chip card was removed from the chip card reader. Since such removal is an expected, normal occurrence in the usage of a chip card, removal of the chip card from the chip card reader could not possibly trigger erasure of the contents of the RAM8, since this would render the chip card useless for its intended purpose, which presumably includes multiple re-use (i.e. insertion into and removal from a chip card reader a number of times). In any event, there is no clear teaching at all in the Sedlak et al reference that it is intended or designed as a card for one-time use, which would be the case if erasure occurred every time the card was removed from the chip card reader.

Therefore, even if the chip card reader, or other components to which the chip card reader is connected, or considered by the Examiner to be the equivalent of a "motherboard," it is clear that the erasure events that are triggered in the chip card disclosed in the Sedlak et al reference cannot be triggered upon mere removal of the chip card from the chip card reader. The erasure events disclosed in the Sedlak et al reference are intended to occur while the chip card is still inserted in the reader and are intended to prevent packing of confidential information from the chip card while it is inserted in the chip card reader.

Therefore, the concept of monitoring insertion of the chip card with respect to a motherboard, as now set forth in independent claims 1 and 3, is meaningless in the context of the chip card disclosed in Sedlak et al.

Equally as importantly, the Sedlak et al reference is completely silent as to what happens *after* erasure of the information from the RAM8 occurs. The term "reset signal" is used in the Sedlak et al reference (somewhat unconventionally) to refer to the *erasure* of information from the RAM8, rather than to restoring its contents (see, for example, column 4, lines 34-39). There is no disclosure whatsoever as to how, or even if, the contents of the RAM8 can be restored after an erasure has occurred. Lastly, again in the context of voltage monitoring, the Examiner has stated that the functioning of the card is inhibited because the RAM8 requires a voltage supply. Presumably the Examiner means that when the chip card in the Sedlak et al reference has been removed from the card reader, it is not possible to enter data into, or read data from, the RAM8. Of course, this is true, but this is trivial since the chip card is not intended to be used in any event without a chip card reader. This is another reason why monitoring a voltage indicating removal of

the security module from the motherboard is meaningful in the context of a security module, but is not meaningful in the context of a chip card. Moreover, even if the chip card in Sedlak et al were removed from the card reader, there is no true "inhibition" of the RAM8, since it would operate as normal if an appropriate battery voltage were applied across the lines GND and V_{cc}. This is why the mere absence of voltage is not the same as "inhibiting." Claims 1 and 3 have been amended to make clear that the inhibiting occurs by virtue of the second function unit (in claim 1) and the unplugged status detection unit (claim 2) occurs by those units being set. As long as those units remain set, operation of the security module truly is inhibited, because even if proper voltage were restored, those units still would be set and therefore still would inhibit operation. In the subject matter of claims 1 and 3, proper operation is restored upon re-commissioning of the security module by, among other things, resetting the second function unit or the unplugged status detection unit.

Therefore, the Sedlak et al reference does not disclose all of the method steps of claim 1, nor all of the elements of claim 3, and does not anticipate either of those claims.

All of the other claims of the application were rejected using the Sedlak et al reference as a primary reference, with reliance upon one or more secondary references. None of the secondary references were relied upon to supply teachings with regard to any of the aforementioned points discussed above, since the Examiner assumed that those teachings or disclosure were already present in the Sedlak et al reference. In view of the above demonstration as to why those method steps and/or circuit components are not present in the Sedlak et al disclosure,

Applicants submit that even if the Sedlak et al reference were modified in accordance with the teachings of one or more of the secondary references cited by the Examiner, the subject matter of the respective dependent claims still would not result. All claims of the application therefore are submitted to be in condition for allowance, and an individual discussion of the teachings of the respective secondary references is not necessary.

Early reconsideration of the application is respectfully requested.

Submitted by,

Steven H. Noll (Reg. 28,982)

SCHIFF, HARDIN LLP
CUSTOMER NO. 26574
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Applicants.

CH1\ 4132993.1